九州大学の学内LANにおける ウェブサーバの分布と傾向について

笠原 義晃*

1 はじめに

近年，インターネットはますます普及し，インターネットの利用法としてのワールドワイドウェブ (以下ウェブ) も完全に定着したように思います。今のところ，ウェブとインターネットは切っても切れない関係にあると言っても過言ではないでしょう。ウェブを閲覧するためのウェブブラウザは，インターネットにつながるパソコンやワークステーション用の OS のみならず，個人情報端末 (PDA) や携帯電話，ゲーム機にも組み込まれています。インターネットでの情報収集にウェブブラウザは必須と言えます。

逆に言うと，インターネットで情報発信をする場合にもウェブを利用するのがよいことになります。九州大学では，今の所学内 LAN で個人が自由にウェブサーバを用意して情報発信できるため，学内に数多くのウェブサーバが稼働しており，研究や趣味の情報を発信していると思います。加えて，ウェブブラウザが一般に普及し，利用者もその操作に慣れているため，プリンタやルータといったネットワークに接続しているさまざまな機器の設定や状態確認にもウェブの仕組みが使われるようになっています。組み込み用のウェブサーバが稼働し，PC 上のウェブブラウザで接続して設定変更などをできる機器が増えているわけです。サーバが動いているのに気づかずに使っている人もいるでしょう。つまり，現在学内のネットワーク上では多数のウェブサーバが稼働し，内外からの接続を待ち続けているということになります。

ウェブサーバが稼働していると，問題になる可能性があります。ウェブサーバに限りませんが，サーバはクライアントからの要求を受け取り，サーバ側で何らかの処理をしてクライアントに応答を返します。通常，クライアントから悪意のある行為 (パスワードファイルを見るとか，機器をクラッシュさせるなど) はできないように，サーバには防御手段が構じてあるのですが，人間が作る物ですから見落しや勘違いなどがある場合もあります。その結果，クライアントから特殊な要求をサーバに送ってサーバを乗っとったり，動作を停止させたりする方法が見つかる場合があります。このような問題点をセキュリティホールと呼びます。もちろん，一般的にそのような問題点は随時修正され，修正されたプログラムが公開されます。しかし，もし利用者が自分の所有する機器でサーバが動いているという事実を知らなければ，新しいプログラムを入れ直すこともなく，セキュリティホールは残ったままになります。

*九州大学情報基盤センター
E-mail : kasahara@nc.kyushu-u.ac.jp

2001 年夏に大発生した CodeRed[1] と呼ばれるプログラムも，このようなセキュリティホールが原因でした。CodeRed は，Windows 2000 (Professional 含む) などに標準で付属している Microsoft Internet Information Server (IIS) というウェブサーバのセキュリティホールを利用し，自身を他の同じ問題を持つサーバに感染させて自己増殖するという機能を持っています。このようにネットワーク上で自己増殖するプログラムをワームと呼びます。このワームがネットワークに放たれた時，インターネット上にはセキュリティホールのある IIS を稼働させている PC が多数あり，ワームはまたたく間に世界中に蔓延しました。このワームは感染するとその PC の力を振り絞って他のホストに攻撃をかけるため，攻撃のためのデータ転送量も大変大きくなります。九州大学でもこのワームが原因で学内 LAN が停止するほどでした。Windows 2000 を標準インストールしても IIS はインストールされませんが，フルインストールしたり，その Windows に特定のソフトウェアをインストールすると，IIS が自動的にインストールされて起動されてしまいます。このため，自分ではサーバを稼働しているつもりがなくても，実は CodeRed が感染する状態になっている PC がたくさんあったのです。IIS 側の問題は既に修正され，修正用のファイルも公開されていますが，発生から 1 年以上経った今でも CodeRed は根絶されておらず，攻撃は少なくなったとは言え日々続いています。また学内でも時々感染するホストが出ています。

CodeRed はほぼ鎮静化しましたが，今後また同じような問題が別のサーバプログラムに対して発生しないとも限りません。このような問題に対策を構じるには，学内でどれくらいどのようなウェブサーバが活動しているかをまず調査する必要があります。情報基盤センターでは，2002 年の 7 月と 8 月に 1 回ずつ，試験的にこの調査を行ないました。本稿では，その結果の概略と，発見された主なウェブサーバに関する情報を提供します。

2　経緯

2002 年 6 月，特に UNIX 系の OS で最も利用されている Apache というウェブサーバに，重大と思われるセキュリティホール[2]が発見されました。発見された時には，このセキュリティホールを利用してそのサーバを乗っ取られる可能性が示唆されました。最終的に，そのセキュリティホールは CodeRed の時ほど簡単には利用できないことがわかりましたが，発見された時には CodeRed の再来になるのではないかと言われた程のインパクトがありました。少なくとも特定の OS(FreeBSD の特定のバージョン) に対して，自己増殖するワームが作成され，インターネット上で活動していることが確認されていました。

Apache は学内でも多数利用されているため，CodeRed の二の舞になる恐れがあり

[1] http://www.microsoft.com/japan/technet/security/virus/default.asp
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0392

ました。しかし，学内でどれくらいApacheが利用されているかは把握されていませんでした。そこで，ウェブサーバに接続した時にサーバから帰ってくる応答を収集し，学内LANにおけるウェブサーバの稼働数やその種類の分布を調査することになりました。

調査は7月15日と8月23日の2回実施されました。また，7月の調査後，問題があると思われるApacheウェブサーバが稼働している支線の支線LAN管理者にそのことを通知しました。

調査には，scanssh[3]というソフトウェアを使用しました。このソフトウェアは元々SSHのバージョン文字列を収集するために開発されたのですが，-p 80というオプションでポート80(ウェブサービスに利用されるポート番号)を指定するとウェブサーバのバージョンを収集するという機能があります。そこで，簡単のため今回はこのソフトウェアを利用しました。このソフトウェアによるサーバのスキャン結果は図1のようになります[4]。

図 1: スキャンの出力

```
   :
133.5.***.110 <refused>
133.5.***.111 <refused>
133.5.***.112 HTTP/1.0 501 Not implemented
133.5.***.113 <refused>
133.5.***.114 <timeout>
133.5.***.115 Server: JC-HTTPD/1.3.7
133.5.***.116 HTTP/1.0 501 Not implemented
133.5.***.117 <timeout>
133.5.***.118 <timeout>
133.5.***.119 <refused>
133.5.***.12 <timeout>
133.5.***.120 <closed>
133.5.***.121 Server: JC-HTTPD/1.3.7
133.5.***.122 Server: JC-HTTPD/1.3.7
133.5.***.123 Server: Microsoft-IIS/4.0
133.5.***.124 Server: Apache/1.3.26 (Unix)
133.5.***.125 <refused>
   :
```

[3] http://www.monkey.org/~provos/
[4] 支線のアドレスは隠しています。

Server: で始まる文字列が，サーバが返したサーバの種類を示しています。サーバが自分の種類を返さなかった場合には，HTTP で既定されているステータスコードが表示されます。また，<refused> は「そのアドレスで機器は稼働しているがウェブサーバは動いていない」，<timeout> は「そのアドレスで機器が稼働していない」，<closed> は「そのアドレスで機器は稼働していてサーバも動いているが，接続直後に切断された」という意味になっています。途中にファイアウォールなどがあると，機器があるのに見えない場合もあります。今回の調査ではファイアウォールの存在は考慮せず，結果を返してきたホストだけを対象としました。

3　結果

3.1　総計

まず，センターからのスキャンに対して応答したホストやウェブサーバの総数を表1に示します。

表 1: ホストとサーバの数

日付	サーバなし	サーバあり	合計	サーバ種別判明	種別不明	合計
7月 15 日	6177	893	7070	788	105	893
8月 23 日	5312	835	6147	731	104	835

九州大学は約 6 万 5 千台の機器が接続可能なアドレス空間を持っており，調査ではそのアドレス全てに対し接続要求が出されました。その結果，7 月には約 7 千台，8 月には約 6 千台の機器が (ウェブサーバの有無にかかわらず) 何らかの応答を返しました。これは実際にセンターに登録されているホストの数よりもかなり少ない結果になっています。ファイアウォール等に保護されている機器は見えませんし，8 月は夏休みだったため電源が落とされている機器も多かったと思います。いずれにしても，これくらいの機器が九大の外からも見えているわけです。

ちなみに，九州大学の全アドレス空間をスキャンするのに要した時間は 12 分程度でした。学外からスキャンする場合はもうちょっと時間がかかると思われますが，いずれにしても非常に短時間でスキャンできるわけです。「誰にも言わずにこっそりサーバを動かしているから見つかる心配はないだろう」という考えは全く間違っていると言えます。ネットワークの高速化は，利便性を高めると同時に，危険性を増す原因にもなっていると言えるでしょう。

3.2 Apacheのバージョン

次に，本来の目的であった「Apacheのバージョン」について見てみます。

まず7月の調査です。7月15日当時，正式に公開されているApacheの最新版は1.3.26と2.0.39でした[5]。これらの最新版で，この調査の時に問題になっていたセキュリティホールが修正されました。これより古いバージョンのサーバにはセキュリティホールが残っていました。

調査の結果，発見された893台のサーバのうち，462台がApacheを名乗り，そのうち最新版を名乗ったサーバは168台でした。つまり，残りの294台はそれより古いバージョンでした。これは95の支線に渡って存在していました。そこで，対応する各支線LAN管理者に対しバージョンアップを勧めるメールを送りました。この時，調査の主眼は古いApacheの駆逐にあったため，その他のサーバについては特に連絡等はされませんでした。

続いて8月の調査です。8月23日当時の最新版は1.3.26と2.0.40でした。調査の結果，発見された835台のサーバのうち，409台がApacheを名乗り，そのうち最新版を名乗ったサーバは250台でした。つまり，残りの159台はそれより古いバージョンでした。以上をまとめると表2のようになります。

表2: Apacheのバージョン

日付	全サーバ数	Apache総数	最新版	それ以外
7月15日	893	462	168	294
8月23日	835 (-58)	409 (-53)	250 (+82)	159 (-135)

2回目での最新版とそれ以外の数の変化を見ると，1回目の調査後の指摘によって古いバージョンがある程度駆逐され，最新版に置き換わった様子がわかります。連絡した結果，不要であるとして停止されたサーバもあったようです。つまり，管理者への連絡は効果があったと言えると思います。しかし，完全に駆逐するには至っておらず，やはりメールで支線LAN管理者に連絡するだけでは完全に古いバージョンを駆逐するのは難しいとも言えます。

3.3 調査の問題点

1回目の調査で見つかった古い(と思われる)Apacheに関して，各支線LAN管理者へ個別に連絡した結果，一部の管理者の方々から返事をいただきました。それらのメールのやりとりを通してこの調査での問題点がわかってきました。

それは，「サーバの返すバージョン文字列だけではセキュリティホールがあるかどう

[5]Apacheは1.x系と2.x系の2つの系統で開発が進められています

か判断できない」ということです。サーバが返すバージョン文字列は，単にサーバがそう主張しているだけですから，管理者がその気になれば任意の文字列を返せます。また，管理者はそこまで手を出していなくても，OS に Apache ウェブサーバが付属しており，かつ OS の開発元がこのバージョン文字列に手を入れている場合が多いのです。

ウェブサーバは OS の管理などに利用される場面が増えており，もともとのプログラムに OS の開発元によって改変が加えられている場合があります。また，Apache の開発元によるバージョンアップに伴う機能拡張により，その OS に付属している設定ファイルが使えなくなる等，機能拡張が邪魔になる場面もあります。このような場合，あるバージョンでセキュリティホールが発見されると，その OS の開発元は Apache のバージョンアップで対応せず，古いバージョンにセキュリティ修正のみを適用します。

今回の調査では，例えば Vine Linux においてバージョンは 1.3.23 のまま修正が施されたサーバ，RedHat Linux において 1.3.22 を修正したサーバ，また古い Debian Linux では 1.3.6 というようなかなり古いサーバを独自に修正し続けていることがわかりました。また，セキュリティ修正が適用される前と後で，ウェブサーバが返すバージョン文字列には変化が無いサーバが多く，スキャンをかけてバージョン文字列を集めても対処済みかどうかがわからないサーバがかなりありました。

このように通常のサーバ応答だけで判断がつかない場合，セキュリティホールがあるかどうかを調べるには，実際に攻撃をかけてみるしかありません。今回の調査では，たまたま手元に疑似攻撃をかけてセキュリティホールの有無を判別できるプログラムがあったため，これを希望する部局のサーバにだけ使用して，本当にセキュリティホールの対策が行われているかどうかを調べることができました。しかし，常にこのような疑似攻撃ツールが手に入るとは限りませんし，疑似といってもセキュリティホールを突くことには変わりがないため，思わぬ障害が出るかもしれません。

この問題は Apache に限った話ではありません。例えば Microsoft IIS でも同様で，先に述べた CodeRed 対策がされたかどうかもバージョン文字列では判別ができません。セキュリティ対策がなされているかを外部から調べる監査ツールを利用して，ある程度は情報収集できます。とは言え，最も正確にそのホストの状況を把握できるのはそのホストの管理者です。各ホストの管理者が，責任と自覚を持ってホストを管理するのが最良の対策と言えるでしょう。

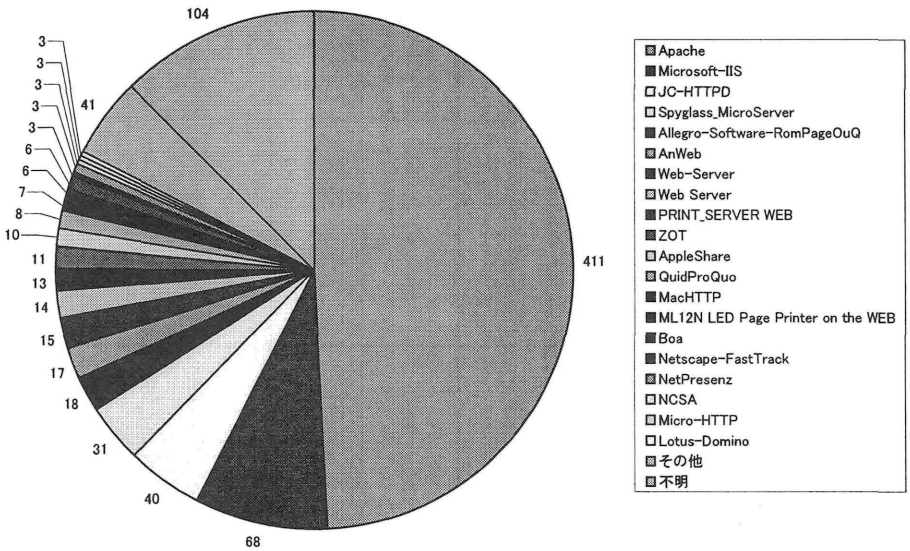
4　Apache 以外のサーバについて

4.1　サーバの種類

当初この調査では Apache のバージョン調査を主眼に置いていたわけですが，収集した情報には他のサーバからの応答も含まれています。そこで，Apache 以外にどの

ようなサーバが発見できたかを集計してみました。集計は，8月23日分の調査結果を元に行いました。サーバの返したバージョン文字列から単純に集計した結果を図2に示します。

図 2: 発見されたサーバの種類



これを見ると，お馴染みのApacheやMicrosoft IISといったサーバ以外に，あまり聞かない名前がたくさんあるのに気づくと思います。JC-HTTPD 40台とか，Spyglass Microserver 31台などです。これだけ見ても正体がわからないため，ひとつひとつ実際にウェブブラウザで接続し，どんなページが表示されるか調べてみました。

その結果，これら見慣れないサーバ名は，プリンタなどの機器に組み込まれたサーバであることが判明しました。学外から接続してみたわけではないため，学外からのアクセスが制限されているかははっきりしませんが，少なくとも他の支線から見えるようになっている機器が多数ありました。プリンタの設定がまるみえなだけでなく，中には設定の変更が可能そうな機器もありました。[6]

見つかったサーバの中で数が多かった物をいくつか紹介します。

- Apache
  - Apache Software Foundation開発のウェブサーバ
  - `http://httpd.apache.org/`
- Microsoft-IIS

[6]大きな声では言えませんが「再起動」のリンクをクリックしてみたらなんの確認もなくいきなり再起動がかかってしまった機器もありました。

  - Microsoft Internet Information Server
  - `http://www.microsoft.com/japan/products/iis/`
- JC-HTTPD
  - silex technology 社のプリンタサーバに内臓される組み込み用ウェブサーバ
  - `http://www.jci.co.jp/japan/support/index.html`
  - プリンタ外付け用，プリンタ内蔵用 (Canon・EPSON) 各種
- Spyglass_Microserver
  - Spyglass 社の小型軽量組み込み用ウェブサーバ
  - `http://www.spyglass.com/`
  - NEC Multiwriter，XEROX Phaser 等のプリンタ
- Allegro-Software-RomPager
  - Allegro Software 社の組み込み用ウェブサーバ
  - `http://www.allegrosoft.com/rpproduct.html`
  - Extreme Summit(ネットワークスイッチ)，EPSON プリンタ，APC(インテリジェント電源) 等
- AnWeb
  - フリーの Windows 用ウェブサーバ
  - `http://www.st.rim.or.jp/~nakata/`
- Web-Server・Web Server
  - 素性不明 (RICOH 製?)
  - RICOH プリンタに組み込み
- PRINT_SERVER_WEB
  - 素性不明
  - CANON LASER SHOT 専用プリントサーバ NetHawk に組み込み
- ZOT
  - Zero One Technology 社のプリントサーバ組み込み
  - `http://www.01tech.com/index1.htm`
  - Planex などに OEM されている
- Microsoft-PWS
  - Microsoft 社のウェブサーバ (Personal Web Server・Peer Web Service)
  - IIS の前身? サポートは既に無し
  - Windows 95 などで動いている
- AppleShare

- Apple MacOS 用商用インターネットサーバソフトウェア群
- http://www.apple.co.jp/applesshareip/

学内 LAN ではこれ以外にもさまざまな種類のサーバが稼働していました。どちらかというと，PC やワークステーションで動作するサーバの方が種類が多く，管理者の趣味・嗜好によってソフトウェアが選択されているのがわかります。それに対し組み込み用サーバは導入した機器に入っているソフトウェアがそのまま使われるため，それほどバリエーションは多くありませんでした。

4.2 サーバの内容

8月 23 日に発見された全てのサーバ 825 台に対して，実際にウェブブラウザでアクセスし，その内容を目視で確認しました。確認時期が最初の調査からだいぶ遅れてしまったため，接続できない機器が 87 台ありました。連休中だったため，プリンタなどは停止していたと思われます。残りも目視による判断のため分類は大雑把ですが，だいたい以下のような内容になっていました。

- 九大関係公開用: 約 300 台
- プリンタ関係: 168 台応答・約 40 台電源断 (サーバ名から判断)
- 初期ページ放置: 83 台
- その他
  - ユーザ認証要求のみ
  - 内輪向け (ウェブメールなど)
  - ファイル一覧が出る
  - 空

この中で「初期ページ放置」というのは，IIS での「工事中」ページや，Apache の「It worked!」など，サーバをインストールした時に自動で設定されるトップページが表示されたサーバを表しています。これらのページを返すサーバは，入れて動かしただけで放置されている場合が多く，セキュリティ上危険な可能性が高いと考えています。

4.3 セキュリティについて

今回，サーバの種類を調査した時に，セキュリティホールに関する情報が出ていないかも調べました。しかし，Apache や IIS のようなメジャーなサーバ以外では，そ

れほど多くの情報は得られませんでした。今の所，プリンタなどの組み込み系サーバの動作を乗っとって悪さをするような人はあまりいないか，見つかっていないようです。組み込み機器はCPUの種類もまちまちで開発環境も一般的で無く，そのような攻撃ツールを開発するのは難しいのかもしれません。

しかし，プリンタなどでサーバが動いているためにプリンタを利用したユーザのユーザ名が漏れていたり，またパスワードの設定がされていないために外部からの設定変更を許している機器がかなりあります。たぶん，利用者は自分が使っているプリンタでウェブサーバが動いている事実すら知らない場合が多いのではないでしょうか。あるIPアドレスがついた機器でウェブサーバが動いているかどうかは，URLにIPアドレスを指定してウェブブラウザでアクセスすればすぐわかるので，確かめてみた方がよいと思います。もしその機器でウェブサーバが動いているとわかり，誰もそれを必要としていないなら，安全のためサーバの機能は止めてしまった方がよいでしょう。

もっと悪い例としては，ウェブブラウザ経由で管理者権限でアクセスできるネットワーク機器が数台見つかっています。すなわち，学外からそのネットワーク機器を操作して，その機器に接続しているネットワークを遮断したり，パケットを操作できるおそれがあります。

よほどのことがない限り，プリンタなどの機器の情報を支線の外から見る必要はないはずです。必要のないサービスは止める，というのは何もワークステーションやPCに限った話ではなく，プリンタなどの機器にも必要な考え方であると言えるでしょう。

5　おわりに

本稿では，2002年7月と8月に行なわれた学内ウェブサーバ全数調査の結果を元に，学内LAN上で稼働しているウェブサーバの種類とその内容について紹介しました。

今回の調査で，学内で利用されているサーバはApacheが大多数を占めており，Microsoft IISは予想よりかなり少ないことがわかりました。CodeRedやNimdaによる大攻勢によってIISの利用を諦めた管理者がかなり多かったのではないかと考えています。Apacheについては，支線LAN管理者へのメール連絡によってある程度最新版への更新をしていただけましたが，やはりそれだけでは不十分で，古いままのサーバも依然として残っています。サーバの返すバージョン文字列を収集するだけでは，セキュリティホールの調査としては不十分であることもわかりました。

また，同時にウェブブラウザでアクセス可能なプリンタ等の機器がかなりの数発見されました。これらの機器は直接セキュリティホールになるという訳ではありませんが，トラブルを未然に防ぐという意味ではあまりよい状況ではないように思います。ウェブに関してだけ言えば，ウェブブラウザを使って簡単にサーバの存在を調べられますので，不審に思ったら試してみるのがよいと思います。たまにはプリンタなどの

取扱説明書に目を通してみるのもよいでしょう。

センターではこれ以降全数スキャンによる調査は行なっていませんが，効果が限定的であるとしても，対策を進めるためには定期的な調査が必要だろうと考えています。ただ，今回はかなりの部分を手作業で行なったため効率が悪かったという問題もあります。自動化を進めれば，定期的な調査により傾向の変化を掴むこともできるようになるでしょう。また，ウェブサーバ以外のサーバ (メールサーバ，DNS サーバ等) についても，同様な調査をする仕組みを用意する必要があると考えています。

調査によって問題点が発見されたとしても，これを解決するには各支線 LAN 管理者，および利用者の協力が不可欠です。センターとしても，電子メールやウェブ，講習会などを通じて，ユーザや管理者への情報提供，啓蒙活動を進めて行きたいと考えています。安全で快適にネットワークを利用できるようにするため，今後とも御協力をお願いします。